AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

1. (currently amended) A method for encrypting a data file content, the method comprising the steps of:

encrypting the data file with a master key;

generating one or more dual-encrypted blocks based on a set of secondary keys, the dual-encrypted blocks contained within the encrypted data file; and

providing the encrypted data file and an attachment file to an authorized user, ~~the attachment file enabling a device to access the data file content once for each secondary key~~ where the attachment file includes a master key and at least two secondary keys so that the data file can be accessed by a device once for each secondary key contained in the attachment file.

2. (original) The method of claim 1 further including the steps of:

randomly generating the master key; and

hiding the master key within a data structure of the attachment file.

3. (original) The method of claim 2 further including the steps of:

creating an odd logarithmic bit integer; and

incrementing the integer by two unit a prime number is found;

said prime number defining the master key.

4. (original) The method of claim 2 further including the step of using an NP-hard program to hide the master key.

5. (original) The method of claim 1 further including the steps of:

selecting one or more continuous blocks to be dual-encrypted;

randomly generating the secondary keys;

generating a duplicate selected block for each secondary key in the set;

generating dual-encrypted blocks based on the duplicate selected blocks and the secondary keys;

inserting the dual-encrypted blocks into the data file.

6. (currently amended) The method of claim 5 further including the steps of:

~~encrypting the secondary keys with the master key~~ encrypting at least one secondary key in the set of secondary keys with the master key, where the set of secondary keys are sequentially ordered;

formatting the encrypted secondary keys as a data structure; and

storing the data structure in the attachment file.

7. (original) The method of claim 6 further including the steps of:

~~encrypting a first secondary key with the master key; and~~

encrypting each secondary key subsequent ~~secondary keys in the set~~ to the at least one secondary key with all preceding secondary keys in the sequentially ordered set of secondary keys, where the at least one secondary key is a first secondary key in the sequentially ordered set; and

encrypting the first secondary key with the master key.

8. (original) The method of claim 1 further including the steps of:

receiving an email message from the attachment file, the message having a status content unique to the attachment file; and

determining whether another message having the status content has already been received.

9. (original) The method of claim 8 wherein the status content defines a current operational state and an identifier for the attachment file.

10. (original) The method of claim 8 further including the step of storing the status content to a data storage medium.

11. (currently amendment) A method for enabling a device to access an encrypted data file content, the method comprising the steps of:

decrypting single-encrypted blocks of the data file with a master key;

decrypting dual-encrypted blocks of the data file with the master key and ~~a~~ ~~secondary key~~ at least one secondary key in a set of secondary keys, where the set of secondary keys contains at least two secondary keys; and

repeating the decryption steps for each secondary key in ~~a~~ the set of secondary keys such that the device is able to access the data file content once for each secondary key in the set.

12. (original) The method of claim 11 further including the step of decrypting the blocks on a block-by-block basis such that the device only has access to the data file content one block at a time.

13. (original) The method of claim 12 further including the step of re-encrypting the single-encrypted blocks with a new master key.

14. (original) The method of claim 13 further including the steps of:

randomly generating the new master key; and

hiding the new master key within a data structure.

15. (original) The method of claim 14 further including the steps of:

creating an odd logarithmic bit integer; and

incrementing the integer by two until a prime number is found;

said prime number defining the new master key.

16. (original) The method of claim 14 further including the step of using an NP-hard problem to hide the new master key.

17. (original) The method of claim 12 further including the step of discarding the dual-encrypted blocks after decryption with the secondary keys.

18. (original) The method of claim 11 further including the step of transmitting an email message to a provider of the encrypted data file, the message having a status content.

19. (original) The method of claim 11 further including the step of adding footprint files to a host system, the footprint files enabling detection of copying of the encrypted data file.

20. (original) The method of claim 11 further including the step of adding footprint data to files contained on a host system, the footprint data enabling detection of copying of the encrypted data file.

21. (new) The method of claim 11 further comprises decrypting the at least one secondary key with the master key, where the set of secondary keys are sequentially ordered and the at least one secondary key is a first key in the sequentially ordered set of secondary keys.

22. (new) The method of claim 21 wherein the step of repeating the decrypting steps further comprises:

decrypting a second key in the sequentially ordered set of secondary keys using the first key; and

decrypting dual-encrypted blocks of the data file with the master key and the second key.

23. (new) The method of claim 22 further comprises:

decrypting a third key in the sequentially ordered set of secondary keys using the first key and the second key; and

decrypting dual-encrypted blocks of the data file with the master key and the third key.

24. (new) The method of claim 21 wherein the step of repeating the decrypting steps further comprises:

decrypting a next secondary key in the sequentially ordered set of secondary keys using each previously decrypted secondary key from the sequentially ordered set of secondary keys; and

decrypting dual-encrypted blocks of the data file with the master key and the next secondary key.